二項方程式を満たす原始根の分布について (解析数論の展望と諸問題)

AUTHOR(S):

竹内, 良平

CITATION:

竹内, 良平. 二項方程式を満たす原始根の分布について (解析数論の展望と諸問題). 数理解析研究所講究録 2001, 1219: 142-150

ISSUE DATE:

2001-07

URL:

http://hdl.handle.net/2433/41267

数理解析研究所講究録 1219 巻 2001 年 142-150

二項方程式を満たす原始根の分布について

竹内 良平 (Ryouhei Takeuchi)
(都立大理・博士課程, Tokyo Metropolitan University)

1. Introduction

1.1 Main Problem

Artin の原始根に関する予想とは,「整数 a に対して, a が -1 や平方数でなければ $a \bmod p$ が原始根となるような素数 p が無限に存在する」という命題が正しいというものである. この命題を次の同値関係に基づいて拡張する.

$$a \text{ が } \bmod p \text{ で原始根} \iff f(X) = X - a \text{ の根が } \bmod p \text{ で原始根}$$

であるから, $f(X)$ として monic で既約な一般の整係数多項式全体を対象にすれば命題は拡張される.

Example 1.) $f(X) = X^2 - X - 1$ に対しては,

$p = 11$: $f(X) = (X-4)(X-8)$, $\mathbb{F}_{11}^{\times} = \langle 8 \bmod 11 \rangle$
$p = 19$: $f(X) = (X-5)(X-15)$, $\mathbb{F}_{19}^{\times} = \langle 15 \bmod 19 \rangle$
$p = 29$: $f(X) = (X-6)(X-24)$, $\times$
$p = 31$: $f(X) = (X-13)(X-19)$, $\mathbb{F}_{31}^{\times} = \langle 13 \bmod 31 \rangle$
$p = 41$: $f(X) = (X-7)(X-35)$, $\mathbb{F}_{41}^{\times} = \langle 7 \bmod 41 \rangle, \langle 35 \bmod 41 \rangle$
$p = 59$: $f(X) = (X-26)(X-34)$, $\mathbb{F}_{59}^{\times} = \langle 34 \bmod 59 \rangle$
$p = 61$: $f(X) = (X-18)(X-44)$, $\mathbb{F}_{61}^{\times} = \langle 18 \bmod 61 \rangle, \langle 44 \bmod 61 \rangle$

ここで扱う拡張された命題を正確に記述する為に必要な記号を定義し, Artin 予想の次のような一般化について考える (R.Takeuchi[6]).

Notation 1. $f(X) \in \mathrm{Irr}(\mathcal{O}) := \{ g(X) \in \mathbb{Z}[X] \mid g(X) \text{ は monic} \wedge \text{既約} \}$ として, 素数 p の集合を $\mathcal{P}$ とする. このとき,

$$\mathrm{Spl}(f) := \{ p \in \mathcal{P} \mid f(X) \bmod p \text{ が異なる一次因子の積に分解する} \},$$
$$N_f := \{ p \in \mathrm{Spl}(f) \mid \exists a \in \mathbb{F}_p^{\times},\ f(a) \equiv 0 \pmod p \ \wedge\ a \bmod p \text{ は原始根} \}.$$

先程の Example 1 では, $f(X) \in \mathrm{Irr}(\mathcal{O})$, $\mathrm{Spl}(f) = \{ p \mid p \equiv \pm 1 \pmod 5 \}$, $N_f = \{11, 19, 31, 41, 59, 61, \ldots\}$ である. そして, 次の命題についてこの文章では考えるこ

とにする.

多項式型 Artin 予想 N_f が有限集合となる『例外多項式』を決定できて, それらは $\mathrm{Irr}(\mathcal{O})$ の中で密度 0 で存在する. 即ち, ほとんどの f に対しては, $f(X) \bmod p$ の異なる $\deg f$ 個の根の中で, 原始根となるものが存在するような素数 $p \in \mathrm{Spl}(f)$ が無限に存在する.

H.W.Lenstra, Jr. も [2] の論文で類似の命題について考察をしている. 特に上の命題で, $\deg f = 1$ と制限すれば original の Artin 予想であり, このときは C.Hooley[1] によって「一般化された Riemann 予想」(GRH と略記) の仮定の下で counting function $\sharp N_f(x) := \sharp\{p \in N_f \mid p \leq x\}$ の大きさが評価されていて, 例外多項式は $X+1, X-k^2$ (-1, 平方数 に対応) のみである (即ち, Artin 予想は正しい) ことが知られている. 当然, $\deg f > 1$ のときの例外多項式も決定したい訳だが, まずは計算機実験と理論的考察により, 次の例外多項式の List を得た.

【 List of exceptional polynomials, deg f $\leq$ 3 】

- $\deg f = 1$

(Φ_2) : $f(X) = X + 1$
(B_1) : $f(X) = X - a^2$

- $\deg f = 2$

(Φ_4) : $f(X) = X^2 + 1$
(Φ_6) : $f(X) = X^2 - X + 1$
$(B_{2,\mathcal{A}})$: $f(X) = (X+a)^2 - b^2X$
$(B_{2,\mathcal{B}})$: $f(X) = X^2 + (a+b)(2a-b)(a-2b)X + (a^2-ab+b^2)^3$
$(B_{2,\mathcal{C}})$: $f(X) = X^2 - 3^{15}5^9(a^2+b^2)(2a^4+6a^3b+13a^2b^2-6ab^3+2b^4)(a^8+6a^7b+17a^6b^2+18a^5b^3+25a^4b^4-18a^3b^5+17a^2b^6-6ab^7+b^8)(61a^{16}+582a^{15}b+2305a^{14}b^2+6030a^{13}b^3+12270a^{12}b^4+15486a^{11}b^5+25187a^{10}b^6+9870a^9b^7+29795a^8b^8-9870a^7b^9+25187a^6b^{10}-15486a^5b^{11}+12270a^4b^{12}-6030a^3b^{13}+2305a^2b^{14}-582ab^{15}+61b^{16})X+3^{30}5^{15}(a^2-ab-b^2)^{30}$

- $\deg f = 3$

$(B_{3,\mathcal{A}})$: $f(X) = X(X+a)^2 - (bX+c)^2$
$(B_{3,\mathcal{B}})$: $f(X) = X(X+a)^2 - k(bX+c)^2$ with $[D_f]' = [k]' \neq 1$
$(B_{3,\mathcal{C}})$: $f(X) = (X+a)^3 - b^3X$ with $[D_f]' = -3$
$(B_{3,\mathcal{D}})$: $f(X) = X^3 - 9k^3X^2 - 27k^6X - 27k^9$

ここで, $a, b, c, k \in \mathbb{Z}$, $f(X) \in \mathrm{Irr}(\mathcal{O})$, D_f で f の判別式, $[m]'$ で $m \in \mathbb{Z}$ の square-free part を表すものとする.

1.2 Bounded Exceptional Condition

上の List で Φ_n は n 番目の円分多項式を表しているが, 円分多項式は十分大きい全ての素数 p に対して mod p での根の位数が n と固定されているので, 必ず例外多項式である. それでは, 他の type の例外多項式が満たす例外性の理由はどのようなものであろうか. 次の例をもとに考察してみる.

Example 2.) $f(X) = X^2 - 2\cdot 3^{15}\cdot 5^9\cdot 61\cdot X + 3^{30}\cdot 5^{15}$ について,

- f は List の $(B_{2,C})$-type において $(a,b) = (1,0)$ と特殊化したものである.
- $[D_f]' = [2^4\cdot 3^{30}\cdot 5^{15}\cdot 11^2\cdot 31^2]' = 5$.
- $p \in \mathrm{Spl}(f) \Leftrightarrow p \equiv \pm 1 \pmod 5$.
- $\alpha := (15 \pm 3\sqrt{5})/2$ とする, このとき f の $\mathbb{C}$ での根は $\alpha^{15} \in \mathbb{Q}(\sqrt{5})$.
- $\sqrt{\alpha} \in \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$ なので, $p \equiv \pm 1 \pmod{15}$ のとき, α は $\mathbb{F}_p^\times$ で平方剰余である.

従って, 任意の $p \in \mathrm{Spl}(f)$ に対して $\gamma := \alpha^{15} \bmod p$ とすると,

$$\begin{cases} \text{(i)} & p \equiv 1 \pmod{15} \Rightarrow & \gamma \text{ は 30 乗剰余である.} \\ \text{(ii)} & p \equiv 4 \pmod{15} \Rightarrow & \gamma \text{ は立方剰余である.} \\ \text{(iii)} & p \equiv 11 \pmod{15} \Rightarrow & \gamma \text{ は 5 乗剰余である.} \\ \text{(iv)} & p \equiv 14 \pmod{15} \Rightarrow & \gamma \text{ は平方剰余である.} \end{cases}$$

以上から, 全ての場合において γ は原始根でない. よって, N_f は有限集合である.

Notation 2.

$$r(a,p) := \begin{cases} [\mathbb{F}_p^\times : \langle a \bmod p\rangle] & (\text{if } a \neq 0 \text{ in } \mathbb{F}_p) \\ \infty & (\text{if } a = 0 \text{ in } \mathbb{F}_p) \end{cases}$$

$$\tilde{r}(a,p) := \begin{cases} r(a,p) \text{ の最小素因数} & (1 < r(a,p) < \infty) \\ r(a,p) & (r(a,p) = 1, \infty) \end{cases}$$

このとき, $r(a,p) = 1 \Leftrightarrow \mathbb{F}_p^\times = \langle a \bmod p\rangle \Leftrightarrow a \bmod p$ は原始根. また, $r(-1,p) = [\mathbb{F}_p^\times : \langle -1\rangle] = (p-1)/2$, $\tilde{r}(a^2,p) = 2$ $(p \nmid a, p \neq 2)$ である.

$f(X) \in \mathrm{Irr}(\mathcal{O})$ に対して, $\mathrm{Spl}(f)$ の元を p_f で表し, 更に γ_i を $f(X) \bmod p_f$ の根とする $(1 \leq i \leq \deg f)$. そして, $r(\gamma_i, p_f) = \infty \Leftrightarrow p_f \mid (f \text{ の定数項})$, であるから $r(\gamma_i, p_f) = \infty$ なる p_f は高々有限個であることがわかる. よって, 十分大きな p_f に対して $\tilde{r}(\gamma_i, p_f)$ の値は $\{1\} \cup \mathcal{P}$ をとる. このことから, f が例外多項式であることを次のようにかけることに注意しておく.

$$\sharp N_f < \infty \iff \exists B \in \mathbb{N}, \text{ s.t. } \forall p_f \geq B, \ \forall i, \ \tilde{r}(\gamma_i, p_f) \in \mathcal{P}.$$

さて, Example 2 でも見たように List にある円分多項式でない例外多項式の例外性

の理由としては, $\mathcal{L}$ という $\mathcal{P}$ の或る有限部分集合が存在して,

$$\bigvee_{l\in\mathcal{L}}\left\{(\gamma_i \text{ は } \mathbb{F}_{p_f}^{\times} \text{で } l \text{ 乗剰余である}) \wedge (p_f \equiv 1 \pmod{l})\right\} \implies$$
$$\bigvee_{l\in\mathcal{L}}\{\tilde{r}(\gamma_i, p_f) = l\} \implies \gamma_i \text{ は } \mathbb{F}_{p_f}^{\times} \text{で原始根でない},$$

であるから, 次の例外多項式である為の十分条件を定義する.

Definition. $f(X) \in \mathrm{Irr}(\mathcal{O})$ が Bounded Exceptional Condition (BEC) を満たすとは, $\mathrm{Spl}(f)$ の元を p_f で表し, 更に γ_i を $f(X) \bmod p_f$ の根とする $(1 \le i \le \deg f)$ とき, $f(X)$ が次を満たすことをいう.

$$\exists B \in \mathbb{N},\ \exists \mathcal{L} = \mathcal{L}(B) : \mathcal{P} \text{ の有限部分集合, s.t. } \forall p_f \ge B,\ \forall i,\ \tilde{r}(\gamma_i, p_f) \in \mathcal{L}.$$

この BEC の定義において Example 2 の多項式は $\mathcal{L}$ として $\{2, 3, 5\}$ がとれることがわかる. また, 奇数番目の円分多項式 $\Phi_{\mathrm{odd}}(X)$ は BEC を満たし, $\mathcal{L}$ として $\{2\}$ がとれる. そして, 先の List で $B_{\deg,*}$ とあるものは全て BEC を満たすことが示せる. これらのことからも例外多項式の特徴付けとして, 次のことを予想 (期待) する.

My Expectation. 円分多項式でない全ての例外多項式は BEC を満たす. 即ち,

$$\{\text{例外多項式}\} = \{\text{円分多項式}\} \cup \{\text{BEC 多項式}\}.$$

2. Results

まずは次数が 2 以下の二項方程式 $X - m$, $X^2 - m$ に対して, BEC を満たすものを全て決定することができた.

Theorem 1. $m \in \mathbb{Z}$, $k \in \mathbb{N}$, $f(X) \in \mathrm{Irr}(\mathcal{O})$ に対して,
(1) $f(X) = X - m$ が BEC を満たす. $\iff m = k^2$
(2) $f(X) = X^2 - m$ が BEC を満たす. $\iff m = -4k^4, -27k^6$

ここでは証明は省略する (cf. [6]). (2) にある $X^2 + 4k^4$ は List の $(B_{2,\mathcal{A}})$-type を $(a, b) = (2k^2, \pm 2k)$ と特殊化したもので, $\mathcal{L} = \{2\}$ がとれる. また, $X^2 + 27k^6$ は List の $(B_{2,\mathcal{B}})$-type を $(a, b) = (k, -k), (k, 2k), (2k, k)$ と特殊化したもので, $\mathcal{L} = \{2, 3\}$ がとれることがわかる. この結果によって, $f(X) = X - m$, $X^2 - m$ に対しては,

"My Expectation" $\implies$ "多項式型 Artin 予想"

であることがわかる.

更に今回は Hooley と同じ手法をとることにより, $f(X) = X^t - m$ の形の二項方程式に対して GRH (もっと正確には, ある種の Kummer 拡大の Dedekind ζ に対する Riemann 予想) を仮定することによって counting function $\sharp N_f(x)$ の大きさが評価でき, その帰結として例外多項式を決定することができた.

Theorem 2. 二項方程式 $f(X)=X^t-m\in \mathrm{Irr}(\mathcal{O})$ に対して,
(1) GRH を仮定すると, 例外多項式は以下のものに限る.
但し, $\tau=\mathrm{ord}_2(t)$, $c\in\mathbb{Z}$: square-free, $k\in\mathbb{N}$ として, $c\,|\,t$ においては c は負の約数もとれるものとする.
i) $\tau=0$ のとき, $X+1$, X^t-ck^2 $(c\,|\,t,\ c\equiv 1 \pmod 4)$
ii) $\tau=1$ のとき, X^2+1, X^t+4k^4, $X^t-27c^3k^6$ $(c\,|\,t,\ 3\nmid c,\ c\equiv 3 \pmod 4)$
iii) $\tau=2$ のとき, X^4+1, $X^t-27c^3k^6$ $(c\,|\,t,\ 3\nmid c,\ c\not\equiv 2 \pmod 4)$
iv) $\tau\geq 3$ のとき, $X^{2^\tau}+1$, $X^t-27c^3k^6$ $(c\,|\,t,\ 3\nmid c)$
(2) また, これらの多項式はすべて例外多項式である.

この結果により, X^t-m の形の例外多項式の List を簡単に作ることが出来る.

Example 3.) 次数 20 以下の X^t-m の形の例外多項式.

$\deg=1$: $X+1$, $X-k^2$
$\deg=2$: X^2+1, X^2+4k^4, X^2+27k^6
$\deg=3$: X^3-k^2, X^3+3k^2
$\deg=4$: X^4+1, $X^4\pm 27k^6$
$\deg=5$: X^5-k^2, X^5-5k^2
$\deg=6$: X^6+4k^4, X^6+27k^6
$\deg=7$: X^7-k^2, X^7+7k^2
$\deg=8$: X^8+1, $X^8\pm 27k^6$, $X^8\pm 216k^6$
$\deg=9$: X^9-k^2, X^9+3k^2
$\deg=10$: $X^{10}+4k^4$, $X^{10}+27k^6$, $X^{10}+3375k^6$
$\deg=11$: $X^{11}-k^2$, $X^{11}+11k^2$
$\deg=12$: $X^{12}-27k^6$, $X^{12}+27k^6$
$\deg=13$: $X^{13}-k^2$, $X^{13}-13k^2$
$\deg=14$: $X^{14}+4k^4$, $X^{14}+27k^6$, $X^{14}-9261k^6$
$\deg=15$: $X^{15}-k^2$, $X^{15}+3k^2$, $X^{15}-5k^2$, $X^{15}+15k^2$
$\deg=16$: $X^{16}+1$, $X^{16}\pm 27k^6$, $X^{16}\pm 216k^6$
$\deg=17$: $X^{17}-k^2$, $X^{17}-17k^2$
$\deg=18$: $X^{18}+4k^4$, $X^{18}+27k^6$
$\deg=19$: $X^{19}-k^2$, $X^{19}+19k^2$
$\deg=20$: $X^{20}\pm 27k^6$, $X^{20}\pm 3375k^6$

この List からもわかるように, Theorem 2 によって二項方程式の中には例外多項式は密度 0 でしか存在しないことがわかる. よって, 二項方程式においては

$$\textbf{GRH} \implies \textbf{“多項式型 Artin 予想”}$$

であり, 更には

$$\textbf{GRH} \implies \textbf{“My Expectation”}$$

であることも Theorem 2 の証明からわかる.

3. Outline of Proof Theorem 2

まず, Theorem 2 (2) での各多項式の例外性は初等的に証明できるのでこれを示そう. 十分大きい $p \in \mathrm{Spl}(f)$ における f の $\mathbb{F}_p^\times$ での根の一つを γ として, それぞれの例外性をみていく.

- $X^{2^\tau}+1$ において, これは円分多項式であるので, γ の位数は常に $2^{\tau+1}$ であるから γ は原始根でない. よって $X^{2^\tau}+1$ は例外多項式である.
- X^t+4k^4 において, $\gamma^t-4k^4\equiv 0 \pmod p$ である. これを変形すると,

$$\gamma \equiv \left(\frac{\gamma^{t/2}+2k^2}{2k}\right)^2 \pmod p$$

であるから, $2 \mid r(\gamma,p)$ であるので γ は原始根でない. よって X^t+4k^4 は例外多項式である.

- X^t-ck^2 において,

$$\gamma \equiv c\left(\frac{k}{\gamma^{(t-1)/2}}\right)^2 \pmod p$$

であり, $p \in \mathrm{Spl}(f) \Rightarrow p \equiv 1 \pmod t$ に注意して, (ここで, $\left(\frac{*}{*}\right)$ は平方剰余記号)

$$\begin{aligned}\left(\frac{c}{p}\right) &= (-1)^{(p-1)(c-1)/4}\left(\frac{p}{|c|}\right)\\ &= (-1)^{p-1}\left(\frac{1}{|c|}\right) \quad [\because\ c \mid t,\ c\equiv 1 \pmod 4]\\ &= 1\end{aligned}$$

であるから, $2 \mid r(\gamma,p)$ であるので γ は原始根でない. よって X^t-ck^2 は例外多項式である.

- $X^t-27c^3k^6$ において, 既約性より $3 \nmid t$ なので $t \equiv \pm 1 \pmod 3$ であり,

$$\gamma \equiv \left(\frac{3ck^2}{\gamma^{(t\mp 1)/3}}\right)^{\pm 3} \pmod p$$

である. また, (ここで, $\left(\frac{*}{*}\right)$ は平方剰余記号)

$$\begin{aligned}p \in \mathrm{Spl}(f) &\Longrightarrow p \equiv 1 \pmod t \ \wedge\ \left(\frac{3c}{p}\right)=1 \quad [\because\ \tau \geq 1]\\ &\Longleftrightarrow p \equiv 1 \pmod t \ \wedge\ \left(\frac{3}{p}\right)(-1)^{(p-1)(c-1)/4}\left(\frac{p}{|c|}\right)=1\\ &\Longrightarrow p \equiv 1 \pmod{2^\tau} \ \wedge\ \left(\frac{-3}{p}\right)(-1)^{(p-1)(c-3)/4}=1 \quad [\because\ c \mid t]\\ &\Longrightarrow \left(\frac{-3}{p}\right)=1 \quad [\because\ \tau \text{と } c \bmod 4 \text{の値}]\\ &\Longleftrightarrow p \equiv 1 \pmod 3\end{aligned}$$

であるから, $3 \mid r(\gamma, p)$ となるので γ は原始根でない. よって $X^t - 27c^3k^6$ は例外多項式である.

以上から, 円分多項式 $X^{2^\tau}+1$ 以外の多項式は BEC の定義で, X^t+4k^4, X^t-ck^2 に対しては $\mathcal{L}$ として $\{2\}$ を, $X^t-27c^3k^6$ に対しては $\mathcal{L}$ として $\{2, 3\}$ をとることができるので, 全て BEC を満たしていることがわかる.

Theorem 2 (1) の証明の方は概略のみを述べることにする (cf. [7]). まずは, 二項方程式 $f(X) = X^t - m \in \mathrm{Irr}(\mathcal{O})$ に対して $m \neq \pm 1$ としておく. そして Hooley の方法を真似て counting function $\sharp N_f(x)$ の大きさを評価したいのであるが, それには次の prime ideal の集合が活躍する.

$$B(x, M) := \left\{ \mathfrak{p} \;\middle|\; \begin{array}{l} \mathfrak{p} \text{ は } K \text{ の prime ideal, } \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p \leq x, \\ p \equiv 1 \pmod{M}, \sqrt[t]{m} \text{ は } \bmod \mathfrak{p} \text{ で原始根.} \end{array} \right\}$$

ここで, $t_0 = \prod_{p \mid t} p$ (core of t) とし, ζ_n で 1 の原始 n 乗根, $K = \mathbb{Q}(\sqrt[t]{m}, \zeta_{t_0})$, $M \in \mathbb{N}$ とする.

そして, この $\sharp B(x, M)$ の大きさは次のように評価されている:

Theorem (L.Murata(1977)). $k \in \mathbb{N}$: square-free, に対して, 全ての $G_{k,M} := K(\zeta_k, \zeta_M, \sqrt[M]{m})$ の形の代数体における GRH を仮定すると,

$$\sharp B(x, M) = \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{[G_{k,M} : K]} \right) \cdot \pi(x) + O\left(\frac{x \log\log x}{\log^2 x} \right).$$

これをもとに $\sharp N_f(x)$ の評価を 3 つの step に分けて行う.

Step 1. Estimate $\sharp N_f(x)$ by $\sharp B(x, t)$

Kummer 拡大の理論を使えば, $\sharp N_f(x)$ が $\sharp B(x, M)$ たちの有限和で表されることがを示せる. そうすれば,

$$\sharp N_f(x) = c_0 \cdot \pi(x) + O\left(\frac{x \log\log x}{\log^2 x} \right)$$

と表されるが, この定数 c_0 を全ての case について計算するのは, M がいろいろ動くため複雑になり非常に大変である. そこで次の proposition を用意する.

Proposition.

$$\frac{1}{\varphi(t_0)[K : \mathbb{Q}(\zeta_{t_0})]} \sharp B(x, t) \leq \sharp N_f(x) \leq \frac{t_0}{\{\varphi(t_0)\}^2 [K : \mathbb{Q}(\zeta_{t_0})]} \sharp B(x, t)$$

この proposition が証明のポイントである. この結果から,

$$c_0 = \lim_{x \to \infty} \frac{\sharp N_f(x)}{\pi(x)} = 0 \iff \lim_{x \to \infty} \frac{\sharp B(x, t)}{\pi(x)} = 0 \overset{\text{GRH}}{\iff} \sum_{k=1}^{\infty} \frac{\mu(k)}{[G_{k,t} : K]} = 0$$

がわかり, 例外多項式を決定するためには $\lim_{x\to\infty}(\sharp N_f(x)/\pi(x)) = 0$ なる f についてだけ考えればよいので $M = t$ の場合だけ計算すればよいことになった.

Step 2. Calculation of $[G_{k,t} : K]$

$$[G_{k,t} : K] = c(m,t,k) \cdot W$$

ここで, $c(m,t,k) = \frac{1}{2}, 1, 2$, $W = \dfrac{\varphi([t,k])k}{\varphi(t_0)(h_m,k)}$, $h_m = \max\{\, k \in \mathbb{N} \mid \sqrt[k]{m} \in \mathbb{Z}\,\}$
(つまり, m は丁度 h_m 乗数) である. また, c の値は k にも依存することに注意しておく.

Step 3. Euler product expansion of $\sum_{k=1}^{\infty}(\mu(k)/[G_{k,t} : K])$

$\sum_{k=1}^{\infty}(\mu(k)/[G_{k,t} : K])$ が 0 になるかどうかの判定は Möbius 関数によって各項の符号が頻繁に変わるため難しい. ところが幸いなことに, この無限和は Euler 積表示を持つ. Step 2 における $c(m,t,k)$ の値を無視すると,

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{W} = \frac{\varphi(t_0)}{\varphi(t)}\prod_{\substack{p\mid t\\ p\nmid h_m}}\left(1-\frac{1}{p}\right)\prod_{\substack{p\nmid t\\ p\mid h_m}}\left(1-\frac{1}{p-1}\right)\prod_{\substack{p\nmid t\\ p\nmid h_m}}\left(1-\frac{1}{p(p-1)}\right)$$

となる. 実際の $\sum_{k=1}^{\infty}(\mu(k)/[G_{k,t} : K])$ の値は $c(m,t,k)$ によって少しずれるが, これは Artin's constant $C = 0.37395\cdots$ の m と t によって定まる非負有理数倍であることがわかる. あとは, $\sum_{k=1}^{\infty}(\mu(k)/[G_{k,t} : K])$ の値が 0 になるような $f(X)$ を Euler 積の各成分をみることによって決定すればよい.

最後に, これからの課題として考えられるものとして,

- 二項方程式以外での例外多項式 (BEC 多項式) の新しい族の発見そして決定.
- "My Expectation" を直接示すことが出来ないか (GRH 仮定の下で)?
- 例外多項式は他に何かよい性質を持つか?

などが挙げられる. それぞれよい問題だと思われる.

参考文献

[1] C.Hooley : *On Artin's Conjecture.* J. reine angew. Math., **225** (1967), 209–220.

[2] H.W.Lenstra, Jr. : *On Artin's Conjecture and Euclid's Algorithm in Global Fields.* Invent. Math., **42** (1977), 201–224.

[3] Leo Murata : *A problem analogous to Artin's conjecture for primitive roots and its applications.* Arch. Math. (Basel) **57** (1991), no.6, 555–565.

[4] J.W.Sander : *On Fibonacci Primitive Roots.* Fibonacci Quarterly, **28** (1990), 79–80.

[5] D.Shanks. : *Fibonacci Primitive Roots.* Fibonacci Quarterly, **10** (1972), 163–168.

[6] R.Takeuchi : *On the polynomial type generalization of "Artin's Conjecture for primitive roots"* (Japanese). Tokyo Metropolitan University, Master thesis (1997/98).

[7] R.Takeuchi : *On the polynomial type Artin's Conjecture for primitive roots* (Japanese). Algebraic number theory and related topics (Japanese) (Kyoto, 2000). Sūrikaisekikenkyūsho Kōkyūroku No. 1154 (2000), 144–154.

〒 192-0397 東京都八王子市南大沢 1 － 1
東京都立大学理学研究科数学教室
E-mail: ryouhei@comp.metro-u.ac.jp